What Is Claimed Is:

1. A method of protecting a program memory device including
    program memory content, wherein the program memory
    content is associated with a previously stored signature,
    the method comprising:

    automatically disconnecting the program memory device
        from a control device that is operationally
        dependent upon the program memory device;

    halting the control device;

    verifying whether a present signature is equivalent to
        the previously stored signature to obtain a
        verification result; and

    based on the verification result, performing one of:

        disabling reading and writing of the program memory
            device; or

        automatically reconnecting the program memory device
            to the control device.

2. The method of Claim 1, wherein the step of verifying
    comprises:

    independently computing a binary content verification of
        the program memory content; and

comparing the previously stored signature with the binary content verification.

3.   The method of Claim 1, wherein the step of independently computing the binary content signature comprises storing the binary content signature in a secure memory device.

4.   The method of Claim 3, wherein the secure memory device is a securely enclosed unit that is tamperproof and that has electrical connections available for connection with the program memory device.

5.   The method of Claim 1, wherein the binary content signature is a binary bit-for-bit copy of the program memory content of the first time period, and the binary content verification is another binary bit-for-bit copy of the program memory content of the second time period.

6.   The method of Claim 1, wherein the protecting is performed automatically and without manual intervention.

7.   The method of Claim 1, wherein the protecting is performed dynamically while the program memory device is being accessed by the control device.

8. The method of Claim 7, wherein the step of disabling reading and writing of the program memory chip comprises maintaining control device stability.

9. The method of Claim 1, further comprising:

    disabling reading and writing of a first portion of the program memory device; and

    maintaining a second portion of the program memory device in an active state.

10. The method of Claim 1, wherein the step of disabling reading and writing of the program memory device comprises preventing unauthorized programming of the program memory device.

11. A method of providing security to a consumer interactive device controlled by a first control device, the method comprising:

    detecting whether the first control device is substituted for a second control device;

    determining whether the second control device comprises one of a secure memory device or a secure memory socket.

12. The method of Claim 11, further comprising:

     determining that the second control device comprises
         neither a secure memory device nor a secure memory
         socket; and

5   suspending operation of the consumer interactive device.

13. The method of Claim 11, wherein the first control device
     comprises one of a secure memory device and a secure
     memory socket.

14. The method of Claim 11, wherein the step of determining
     comprises calculating a program memory signature for an
     initial module in a distributed processor of the control
     device.

15. The method of Claim 11, wherein the consumer interactive
     device is one of:

     a gaming apparatus;

     a slot machine;

20   an automatic teller machine;

     currency acceptor; or

     vending apparatus.

16. A secure memory device comprising:

an electrically accessible memory configured to store a
binary image of a program memory device in
communication with a control device, wherein the
control device controls computational operations of
a consumer interactive device; and

a tamperproof construction configured to detect altering
of the binary image.

17. The secure memory device of Claim 16, wherein the binary
image is a program memory signature of the program memory
device.

18. The secure memory device of Claim 16, wherein the secure
memory device is electrically accessible only to a
program memory device connection.

19. The secure memory device of Claim 16, wherein the
tamperproof construction is further configured to
initiate operations to disable reading and writing of the
program memory device and to disable operation of the
consumer interactive device.

20. A secure memory socket comprising:

an integrated circuit socket capable of accepting a
program memory device in communication with a

control device, wherein the control device controls computational operations in a consumer interactive device; and

a tamperproof construction configured to detect altering of the program memory device.

21. The secure memory device of Claim 20, wherein the secure memory socket is capable of accepting only a program memory device connection.

22. The secure memory device of Claim 20, wherein the tamperproof construction is further configured to initiate operations to disable reading and writing of the program memory device to disable operation of the consumer interactive device.

23. A method of monitoring execution of a program memory, wherein the program memory is accessed by a controlling program of a consumer interactive device, the method comprising:

determining bounds of a contiguous block of memory accessible by the controlling program;

monitoring addresses accessed by the controlling program during execution of the controlling program to determine actually accessed addresses; and

determining whether the actually accessed addresses are outside the bounds of the contiguous block of memory.

5 24. The method of Claim 23, further comprising:

determining that the actually accessed addresses are outside the bounds of the contiguous block of memory;

disabling reading of the program memory; and

10 disabling operation of the consumer interactive device.

25. The method of Claim 23, wherein the method is performed dynamically while the controlling program is in use.

15 26. A computer-readable medium carrying one or more sequences of one or more instructions for protecting a program memory device including program memory content, wherein the program memory content is associated with a previously stored signature, the one or more sequences of

20 one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

automatically disconnecting the program memory device from a control device that is operationally

25 dependent upon the program memory device;

halting the control device;

verifying whether a present signature is equivalent to the previously stored signature to obtain a verification result; and

5   based on the verification result, performing one of:

disabling reading and writing of the program memory device; or

automatically reconnecting the program memory device to the control device.

10

27. The computer-readable medium of Claim 26, wherein the verifying step further causes the processor to carry out the steps of:

independently computing a binary content verification of the program memory content; and

15   comparing the previously stored signature with the binary content verification.

28. The computer-readable medium of Claim 26, wherein the

20   step of independently computing the binary content signature comprises storing the binary content signature in a secure memory device.

29. The computer-readable medium of Claim 28, wherein the
     secure memory device is a securely enclosed unit that is
     tamperproof and that has electrical connections available
     for connection with the program memory device.

5

30. The computer-readable medium of Claim 26, wherein the
     binary content signature is a binary bit-for-bit copy of
     the program memory content of the first time period, and
     the binary content verification is another binary bit-
     for-bit copy of the program memory content of the second
     time period.

10

31. The computer-readable medium of Claim 26, wherein the
     protecting is performed automatically and without manual
     intervention.

15

32. The computer-readable medium of Claim 27, wherein the
     protecting is performed dynamically while the program
     memory device is being accessed by a control device that
     is operationally dependent upon the program memory
     device.

20

33. The computer-readable medium of Claim 32, wherein the
     step of disabling reading and writing of the program

memory chip further causes the processor to carry out the step of maintaining control device stability.

34. The computer-readable medium of Claim 26, wherein the instructions further cause the processor to carry out the steps of:

   disabling reading and writing of a first portion of the program memory device; and

   maintaining a second portion of the program memory device in an active state.

35. The computer-readable medium of Claim 27, wherein the step of disabling reading and writing of the program memory device further cause the processor to carry out the step of preventing unauthorized programming of the program memory device.